



**Становище № 15/2026 относно  
критериите за сертифициране  
Europrivacy във връзка с тяхното  
одобряване от Комитета като  
Европейски печат за защита на данните,  
който да се използва като инструмент за  
предаване на данни съгласно членове 42  
и 46 от ОРЗД**

Прието на 15 април 2026

# Съдържание

|                                                                                                                                            |           |
|--------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1 Кратко изложение на фактите .....</b>                                                                                                 | <b>5</b>  |
| <b>2 Оценка.....</b>                                                                                                                       | <b>6</b>  |
| 2.1 Обхват на механизма за сертифициране и обект на оценката (ОНО) .....                                                                   | 7         |
| 2.2 Операции по обработване .....                                                                                                          | 8         |
| 2.3 Принципи на обработването на данни .....                                                                                               | 8         |
| 2.4 Общи задължения на администраторите и обработващите лични данни .....                                                                  | 9         |
| 2.5 Права на субектите на данни .....                                                                                                      | 9         |
| 2.6 Технически и организационни мерки и оценка на рисковете за правата и свободите на субектите на данни .....                             | 10        |
| 2.7 Критерии за доказване на наличието на подходящи гаранции за предаването на лични данни .....                                           | 11        |
| <b>3 Допълнителни критерии за Европейския печат за защита на данните, който да се използва като инструмент за предаване на данни .....</b> | <b>11</b> |
| <b>4 Заключение/препоръки.....</b>                                                                                                         | <b>12</b> |
| <b>5 Заключителни бележки .....</b>                                                                                                        | <b>13</b> |

## Европейският комитет по защита на данните,

като взе предвид член 63, член 64, параграф 2 и членове 42 и 46 от Регламент 2016/679/ЕС на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (наричан по-нататък „ОРЗД“),

като взе предвид Споразумението за Европейското икономическо пространство (наричано по-нататък „ЕИП“), и по-специално приложение XI и протокол 37 към него, изменени с Решение № 154/2018 на Съвместния комитет на ЕИП от 6 юли 2018 г.<sup>1</sup>,

като взе предвид членове 10 и 22 от своя Правилник за дейността,

- 1 Държавите членки, надзорните органи, Европейският комитет по защита на данните (наричан по-нататък „ЕКЗД“ или „Комитетът“) и Европейската комисия насърчават, особено на равнището на Съюза, създаването на механизми за сертифициране на защитата на данните (наричани по-нататък „механизми за сертифициране“) и на печати и маркировки за защита на данните с цел да се демонстрира спазването на ОРЗД при операциите по обработване от страна на администраторите и обработващите лични данни, като се отчитат конкретните нужди на микропредприятията, на малките и на средните предприятия<sup>2</sup>. Освен това създаването на механизми за сертифициране може да повиши прозрачността и да даде възможност на субектите на данни да оценяват нивото на защита на данните на съответните продукти и услуги<sup>3</sup>.
- 2 Освен спазването на ОРЗД от администраторите или обработващите лични данни, към които се прилага той, може да се установяват механизми за сертифициране, печати или маркировки за защита на данните, одобрени съгласно член 42, параграф 5 от ОРЗД, с цел да се демонстрира наличието на подходящи гаранции, осигурени от администраторите и обработващите лични данни, които не са обект на ОРЗД съгласно член 3, в рамките на предаването на лични данни на трети държави или международни организации (наричани по-нататък „вносители на данни“) съгласно условията, посочени в член 46, параграф 2, буква е) от ОРЗД<sup>4</sup>.
- 3 Сертифицирането, което ще се използва като инструмент за предаване на данни, представлява нов механизъм за предаване, въведен с член 46 от ОРЗД, за да се гарантира, че при липса на решение съгласно член 45, параграф 3 администратор или обработващ лични данни по ОРЗД (наричан по-нататък „износител на данни от ЕИП“) може да предава лични данни към трета държава или международна организация само ако са предоставени подходящи гаранции и при условие че са налице подлежащи на изпълнение права на субектите на данни и ефективни правни средства за тяхната защита. По-конкретно, съгласно член 46, параграф 2, буква е) от ОРЗД механизъм за сертифициране, одобрен в съответствие с член 42 от ОРЗД, може да предоставя тези подходящи гаранции, ако е придружен от обвързващи и подлежащи на изпълнение ангажименти от страна на вносителите на данни да прилагат подходящите гаранции, включително по отношение на правата на субектите на данни. Критериите за

<sup>1</sup> Позоваванията на „държави членки“ в настоящото становище следва да се разбират като позовавания на „държавите — членки на ЕИП“.

<sup>2</sup> Член 42, параграф 1 от ОРЗД.

<sup>3</sup> Съображение 100 от ОРЗД.

<sup>4</sup> Вж. член 42, параграф 2 от ОРЗД.

сертифициране са неразделна част от механизма за сертифициране. Поради това в ОРЗД се изисква критериите за национален механизъм за сертифициране да бъдат одобрени от компетентния надзорен орган (член 42, параграф 5 и член 43, параграф 2, буква б) от ОРЗД) или в случай на Европейски печат за защита на данните — от ЕКЗД (член 42, параграф 5 и член 70, параграф 1, буква о) от ОРЗД).

- 4 Когато надзорен орган (наричан по-нататък „НО“) възнамерява да предложи на ЕКЗД да одобри Европейски печат за защита на данните съгласно член 42, параграф 5 от ОРЗД, той следва да заяви намерението на собственика на схемата да предложи механизма за сертифициране във всички държави членки. В този случай основната роля на ЕКЗД е да гарантира последователното прилагане на ОРЗД посредством механизма за съгласуваност, посочен в членове 63, 64 и 65 от ОРЗД. В тази връзка, ЕКЗД одобрява критериите за сертифициране съгласно член 64, параграф 2 от ОРЗД..
- 5 Европейският печат за защита на данните, одобрен съгласно член 42, параграф 5 от ОРЗД, установен с цел да се демонстрира наличието на подходящи гаранции, предоставени от вносителите на данни, заедно с обвързващите и подлежащи на изпълнение ангажименти, служи като инструмент, в който може да бъде обхванато предаването на данни от всички държави — членки на ЕИП, към трети държави или международни организации<sup>5</sup>.
- 6 При преценката на механизъм за сертифициране, който да се използва като инструмент за предаване на данни, оценката на ЕКЗД се извършва въз основа на „Насоки 1/2018 относно сертифицирането и определянето на критериите за сертифициране в съответствие с членове 42 и 43 от Регламента“ (наричани по-нататък „Насоките“) и допълнението към тях, съдържащо „Насоки за оценка на критериите за сертифициране“ (наричано по-нататък „допълнението“), както и въз основа на „Насоки 07/2022 относно сертифицирането като инструмент за предаване на данни“ (наричани по-нататък „Насоки относно сертифицирането като инструмент за предаване на данни“).
- 7 ЕКЗД признава, че всеки механизъм за сертифициране следва да се разглежда отделно и не засяга оценяването на който и да е друг механизъм за сертифициране.
- 8 Механизмите за сертифициране, които се използват като инструмент за предаване на данни, следва да позволяват на вносителите на данни да демонстрират наличието на подходящи гаранции, за да се гарантира, че нивото на защита на физическите лица, предвидено в ОРЗД, няма да бъде нарушено, когато предаваните лични данни се обработват извън ЕИП<sup>6</sup>. Следователно неговите критерии следва да отразяват надлежно изискванията и принципите относно защитата на личните данни, заложиени в ОРЗД, за да се гарантира, че защитата на личните данни, осигурявана съгласно ОРЗД, остава непроменена<sup>7</sup>.
- 9 Същевременно, собственикът на схемата следва да гарантира съгласуваността и съответствието на механизма за сертифициране с всички включени или използвани стандарти и практики за сертифициране по ISO.
- 10 В резултат на това сертифицирането следва да носи допълнителна полза за вносителите на данни, като подпомага въвеждането на стандартизирани и конкретно определени организационни и технически мерки, с които да се докаже, че са въведени подходящи гаранции при обработването на лични данни, получени от износители на

<sup>5</sup> Насоки на ЕКЗД 07/2022 относно сертифицирането като инструмент за предаване на данни, версия 2.0, приети на 14 февруари 2023 г., точка 30.

<sup>6</sup> Член 44 от ОРЗД.

<sup>7</sup> Вж. Съобщение на Комисията до Европейския парламент и Съвета *Обмен и защита на личните данни в един глобализиран свят*, COM(2017) 7 final, стр. 4.

данни от ЕИП. Във връзка с това ЕКЗД припомня, че обектът на сертифицирането, който съвпада с обекта на оценката (ОНО) по време на сертифицирането, обикновено следва да бъде обработването на данни, предадени на вносителя на данните в третата държава, и транзитното им преминаване, ако то се извършва под контрола на същия вносител<sup>8</sup>.

- 11 Сертификатите ще носят също така добавена стойност за износителя на данни, който може да реши да се позове на сертификата, получен от вносителя на данни, като инструмент за предаване на лични данни съгласно член 46, параграф 2, буква е) от ОРЗД и като елемент за доказване на спазването на задълженията, например съгласно член 24, параграф 3 или член 28, параграф 5 от ОРЗД<sup>9</sup>.
- 12 Във връзка с това ЕКЗД припомня, че износителят на данни, който иска да използва сертификат като подходяща гаранция съгласно член 46, параграф 2, буква е) от ОРЗД, е длъжен да провери дали сертификатът, на който възнамерява да разчита, е ефективен с оглед на характеристиките на планираното обработване. За тази цел износителят трябва да провери валидността и срока на действие на издадения сертификат, дали той обхваща конкретното предаване на данни, което трябва да се извърши, и дали транзитното преминаване на лични данни попада в обхвата на сертификата, както и дали става въпрос за последващи предавания и дали за тях е предоставена подходяща документация<sup>10</sup>.
- 13 Освен това износителят на данни трябва да провери дали сертифициращият орган, който издава сертификата, е акредитиран от национален орган по акредитация или от компетентен надзорен орган. Също така износителят на данни следва да посочи използването на сертифицирането като инструмент за предаване на данни в договора за обработване на данни по член 28 от ОРЗД в случай на предаване на данни от администратор на обработващ лични данни или в договора за обмен на данни с вносителя на данни в случай на предаване на данни от администратор на администратор<sup>11</sup>. Той трябва също да изпълни конкретните задължения, предвидени в член 13, параграф 1, буква е) от ОРЗД, по-специално да информира субекта на данните за използваните подходящи гаранции, т.е. в случай на сертифициране съгласно член 46, параграф 2, буква е) от ОРЗД да информира за сертификата, получен от вносителя съгласно конкретен механизъм за сертифициране, както и за начините за получаване на копие от сертификата и от гаранциите, съдържащи се в критериите за сертифициране, или където са били предоставени на разположение.
- 14 ЕКЗД приветства усилията, положени от собствениците на схеми, за разработване на механизми за сертифициране, които представляват практически и потенциално разходно ефективни инструменти за гарантиране на по-голяма съгласуваност с ОРЗД и насърчаване на правото на неприкосновеност на личния живот и защита на данните на субектите на данни посредством повишаване на прозрачността.
- 15 ЕКЗД припомня, че сертифицирането е доброволен инструмент за отчетност и че придържането към механизъм за сертифициране не възпрепятства надзорните органи да изпълняват своите задачи и правомощия съгласно ОРЗД и съответното национално законодателство. В рамките на сертифицирането, което се използва като инструмент за предаване на данни, както и по-специално по отношение на спазването на

<sup>8</sup> Вж. Насоки на ЕКЗД 07/2022 относно сертифицирането като инструмент за предаване на данни, версия 2.0, приети на 14 февруари 2023 г., точка 16.

<sup>9</sup> Насоки 72022 относно сертифицирането като инструмент за предаване на данни, точка 5.

<sup>10</sup> Насоки 7/2022 относно сертифицирането като инструмент за предаване на данни, точка 20.

<sup>11</sup> Пак там.

задълженията, поети като обвързващи и подлежащи на изпълнение ангажименти от вносителите на данни спрямо износителите на данни чрез договорни или други правно обвързващи инструменти, това означава да се прилагат подходящите гаранции, предвидени в механизма за сертифициране, включително по отношение на правата на субектите на данни.

- 16 Настоящото становище има за цел да се гарантира последователното прилагане на ОРЗД, включително от страна на НО, администраторите и обработващите лични данни, с оглед на основните елементи, които трябва да бъдат установени в механизмите за сертифициране. По-конкретно, настоящото становище има за цел да се оценят критериите за сертифициране, които се предвижда да бъдат използвани като инструмент за предаване на данни от вносителите на данни. Поради това, ЕКЗД разглежда в него въпроси като обхвата, приложимостта и относимостта на критериите при предаване на данни от всички държави — членки на ЕИП, и/или от който и да е износител на данни, попадащ в приложното поле на ОРЗД.
- 17 Становището на ЕКЗД е съсредоточено единствено върху критериите за сертифициране. Комитетът може да поиска подробна информация относно методите на оценка, за да може да прецени напълно проверимостта на критериите в рамките на своето становище по въпроса. Това обаче не обхваща каквото и да било одобрение на такива методи на оценка.
- 18 Становището на ЕКЗД следва да се приеме съгласно член 64, параграф 2 от ОРЗД във връзка с член 10, параграф 2 от Правилника за дейността на ЕКЗД в срок от осем седмици от първия работен ден, след като председателят и компетентният надзорен орган са взели решение, че досието е пълно. По решение на председателя този срок може да бъде удължен с още шест седмици с оглед на сложността на въпроса. Ако в становището на ЕКЗД се стигне до заключението, че въпросните критерии не могат да бъдат одобрени, НО може да ги представи отново за одобрение, след като бъдат взети предвид опасенията, изразени в първоначалното становище на ЕКЗД,

**прие следното становище:**

## **1 Кратко изложение на фактите**

- 19 В съответствие с член 42, параграф 2 и член 46, параграф 2, буква е) от ОРЗД, Насоки 1/2018 и Насоки 7/2022 относно сертифицирането като инструмент за предаване на данни, Европейският център за сертифициране и поверителност (наричан по-нататък „собственик на схемата“) е изготвил версия 82 на Europrivacy (наричани по-нататък „критерии за сертифициране“).
- 20 ЕКЗД припомня, че вече е одобрил критериите за сертифициране Europrivacy (версия 60) на 10 октомври 2022 г., като е издал Становище 28/2022 на ЕКЗД като Европейски печат за защита на данните съгласно член 42, параграф 5 от ОРЗД, чиято цел е да се демонстрира спазването на ОРЗД съгласно член 42, параграф 1 от ОРЗД. Тази схема не представляваше сертифициране по смисъла на член 46, параграф 2, буква е) от ОРЗД, предназначено за предаване на данни.
- 21 На 29 януари 2026 г. Надзорният орган на Люксембург (наричан по-нататък „НО-Люксембург“) представи пред ЕКЗД актуализирана версия на вече одобрените критерии за сертифициране Europrivacy като критерии за сертифициране за Европейски печат за защита на данните с разширен обхват, включващ по-специално заявителите, попадащи в приложното поле на член 3, параграф 2 от ОРЗД, както и други изменения, засягащи

основните критерии за сертифициране (версия 82). ЕКЗД прие Становище 14/2026 относно настоящата актуализирана версия (версия 82) на критериите за сертифициране Europrivacy, чиято цел е да се демонстрира спазването на ОРЗД съгласно член 42, параграф 5.

- 22 На същата дата НО- Люксембург, представи пред ЕКЗД и допълнителен набор от критерии за сертифициране („Разширение на схемата за сертифициране Europrivacy с цел сертифициране на вносители на данни съгласно член 46“), предназначен да се използва като инструмент за предаване на данни съгласно член 46, параграф 2, буква е) от ОРЗД, с оглед на одобряването му съгласно член 64, параграф 2 от ОРЗД.
- 23 Решението относно пълнотата на досието бе взето на 31 март 2026 г.

## 2 Оценка

- 24 ЕКЗД направи оценка на критериите за сертифициране, предназначени да се използват като инструмент за предаване на данни от вносителите на данни, с оглед на тяхното одобряване съгласно член 42, параграф 5 във връзка с член 46, параграф 2, буква е) от ОРЗД, в съответствие със структурата, предвидена в приложение 2 към Насоки 1/2018 (наричано по-нататък „приложението“), допълнението към него и Насоките относно сертифицирането като инструмент за предаване на данни<sup>12</sup>.
- 25 Комитетът подчертава, че в съответствие с условията, посочени в член 42, параграф 2 и член 46, параграф 2, буква е) от ОРЗД, настоящата схема е предназначена да се използва като инструмент за предаване на данни и следователно сертификатите, издадени съгласно схемата, могат да бъдат използвани от износителите на данни по смисъла на глава V от ОРЗД (т.е. от администратори или обработващи лични данни, които не са обект на ОРЗД за даденото обработване<sup>13</sup>) за прехвърлянето на лични данни към сертифицирани вносители на данни, които не са обект на ОРЗД съгласно член 3<sup>14</sup>. Това означава, че предаването на лични данни на вносителя на данни в третата държава може да се осъществи едва след като същият вносител е бил сертифициран и е подписал обвързващи и подлежащи на изпълнение ангажименти спрямо износителя на данни от ЕИП за прилагане на подходящите гаранции, предвидени в критериите за сертифициране, при обработването на предадените лични данни в обхвата на ОНО, включително по отношение на правата на субектите на данни.
- 26 В рамките на настоящото становище и с оглед на одобряването на критериите за сертифициране Europrivacy, предназначени като инструмент за предаване на данни, ЕКЗД оцени документите „Предварителни проверки и контрол на заявлението и обекта на оценката за вносителите на данни (ADI)“; „Основни критерии Europrivacy по ОРЗД за вносителите на данни (GI)“; „Проверки и контрол на техническите и организационните мерки (T)“.
- 27 По отношение на процеса на сертифициране, с оглед на спецификата на сертифицирането, което ще се използва като инструмент за предаване на данни, ЕКЗД подчертава необходимостта от висока степен на прозрачност и приветства разясненията, предоставени в това отношение в схемата за сертифициране Europrivacy, съгласно които „предаването на данни не може да започне, преди да бъде

<sup>12</sup> Вж. по-специално: раздели 3 и 4 от Насоки 07/2022.

<sup>13</sup> Вж. Насоки 05/2021 на ЕКЗД относно взаимодействието между прилагането на член 3 и разпоредбите, свързани с международното предаване на данни съгласно глава V от ОРЗД, версия 2.0, приети на 14 февруари 2023 г., точка 9.

<sup>14</sup> Член 42, параграф 2 от ОРЗД.

извършено сертифицирането“. Във връзка с това ЕКЗД потвърждава, че преди да се осъществи предаването на лични данни, „оценката може да бъде извършена въз основа на лични данни, които не са обект на ОРЗД, или въз основа на нелични данни. При необходимост е възможно да се използват фиктивни данни за оценка на конкретни критерии“, като след започването на предаването на данни „одиторът прави повторна оценка на тези критерии при следващия одит за наблюдение“<sup>15</sup>.

- 28 ЕКЗД припомня, че може да се наложи да бъдат направени някои корекции в процедурата за акредитация на сертифициращите органи по отношение на сертифицирането като инструмент за предаване на данни в съответствие с Насоките относно сертифицирането като инструмент за предаване на данни<sup>16</sup>. Този въпрос обаче не е разгледан в настоящото становище, тъй като не попада в компетентността на ЕКЗД.
- 29 ЕКЗД припомня също така, че в съответствие с член 42, параграф 8 от ОРЗД, и по-специално в случаите, когато сертифицирането се използва като инструмент за предаване на данни в съответствие с член 13, параграф 1, буква е) от ОРЗД, критериите за сертифициране трябва да бъдат предоставени на разположение на субектите на данни, чиито лични данни ще бъдат предадени въз основа на сертификата, предоставен на вносителя на данните.
- 30 Комитетът отбелязва, както е пояснено в определенията на схемата, че позоваванията на „компетентни органи за защита на данните“ в цялата схема имат значението на органи за защита на данните в ЕИП <sup>17</sup>.
- 31 Комитетът отбелязва също така, че позоваванията на „приложимото право“ и „правото на трета държава“ „се отнасят до законодателството, приложимо към заявителя и/или към личните данни, обработвани в обекта на оценката, доколкото това законодателство не налага ограничения върху правата за защита на данните, които надхвърлят необходимото и пропорционалното в едно демократично общество за постигане на някоя от целите, изброени в член 23, параграф 1 от ОРЗД, пропорционално е на преследваната цел, зачита същността на правото на защита на данните и предвижда конкретни мерки за защита на основните права и интереси на субектите на данни“.

## 2.1 Обхват на механизма за сертифициране и обект на оценката (ОНО)

- 32 Разширението на схемата за сертифициране Europrivacy с цел сертифициране на вносители на данни съгласно член 46 е предвидено да се използва в съответствие с член 42, параграф 2 и член 46, параграф 2, буква е) от ОРЗД от вносители на данни, намиращи се извън ЕИП, които не са обект на ОРЗД съгласно член 3, с цел да се демонстрира наличието на подходящи гаранции в рамките на предаването на лични данни към трети държави или към международни организации. Поради това обхватът се различава от този на сертифицирането Europrivacy по член 42, параграф 1, посочен

<sup>15</sup> Вж. Разширение на схемата за сертифициране Europrivacy™/® с цел сертифициране на вносители на данни съгласно член 46 от ОРЗД, EP-CS.1.DI, т. 6.1.

<sup>16</sup> Насоки 07/2022, раздел 2.

<sup>17</sup> Вж. определението, предвидено в критериите Europrivacy за „компетентен НО“: „Компетентен орган за защита на данните“ означава органите за защита на данните в ЕИП. Като цяло това се отнася за националните органи за защита на данните, които са компетентни да следят за спазването на изискванията при обработването на лични данни от страна на обекта на оценката. В случай на сертифициране по ОРЗД, издадено на вносител на данни съгласно член 46 от ОРЗД, компетентният орган за защита на данните е органът на износителя на данни в ЕИП, освен при подаване на жалба, когато компетентен е всеки орган в ЕИП.

в точка 3 от настоящото становище, тъй като в него се предвиждат конкретни критерии, които да се прилагат и спазват при извършването на сертифициране Europrivacy на заявители (администратори или обработващи лични данни), намиращи се извън ЕИП, които възнамеряват да действат в качеството си на вносители на данни.

- 33 Схемата за сертифициране Europrivacy като инструмент за предаване на данни е предназначена да се прилага както при единично предаване, така и при набор от предавания на данни, когато последните са тясно свързани помежду си. Схемата за сертифициране съдържа критерии за сертифициране на операции по обработване в рамките на обекта на оценката (ОНО), извършвани върху лични данни, предавани на вносителя на данните, включително транзитното преминаване, когато то се осъществява под контрола на същия вносител<sup>18</sup>.
- 34 ЕКЗД отбелязва, че обхватът на тази схема за сертифициране не включва съвместни администратори и че, когато „съвместното администриране е включено в ОНО, тогава сертифициращият орган трябва да откаже извърши сертифициране“<sup>19</sup>.

## 2.2 Операции по обработване

- 35 В критериите за сертифициране се разглеждат съответните компоненти на операциите по обработване на лични данни, предавани в рамките на обхвата на ОНО. По-конкретно, в критериите за сертифициране се предвиждат гаранции за обработването на специални категории лични данни (раздел Gl.2 от критериите „Обработване на специални категории данни“). Във връзка с това Комитетът приветства факта, че съгласно критериите за сертифициране (критерий G.2.1.3 „Допълнителни гаранции при обработването на специални категории лични данни“) се изисква също така заявителят да въведе допълнителни ограничения и гаранции, съобразени със специфичния характер на данните и съответните рискове, когато обработването засяга специални категории лични данни.

## 2.3 Принципи на обработването на данни

- 36 Критериите за сертифициране в раздел Gl.1 отговарят в достатъчна степен на принципите за защита на данните, съответстващи на предвидените в член 5 от ОРЗД, с цел да се гарантира, че обработването на данни в ОНО е законосъобразно и пропорционално.
- 37 По-конкретно, в критерия за сертифициране Gl.1.1.2 са разгледани надлежно принципът за ограничаване на целта и съответните задължения на заявителя за спазването му. ЕКЗД отбелязва, че предадените лични данни могат да се обработват единствено за целите, за които са били предадени. В критерия за сертифициране Gl.1.1.3, в съответствие с действащите стандартни договорни клаузи, приети от Европейската комисия<sup>20</sup>, се определят единствените изключения, при които данните могат да бъдат обработвани по-нататък за цели, различни от тези, за които са били събрани първоначално (а именно: за предварително информирано съгласие, законово задължение, жизненоважни интереси на субектите на данни и правни искиове).

<sup>18</sup> Вж. критерии за сертифициране Gl.11.1.5 и Gl.11.1.6.

<sup>19</sup> Разширение на схемата за сертифициране Europrivacy™/® с цел сертифициране на вносители на данни съгласно член 46 от ОРЗД, EP-CS.1.DI, точка 3.2.2., където също така ясно се посочва, че „съвместното администриране е изключено от обхвата на схемата за заявители по член 46“.

<sup>20</sup> Решение за изпълнение (ЕС) 2021/914 на Комисията от 4 юни 2021 г. относно стандартни договорни клаузи за предаването на лични данни на трети държави съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета.

- 38 ЕКЗД отбелязва също, че заявителят е длъжен да представи писмена оценка, за да гарантира, че законодателството и практиката в третата държава не го възпрепятстват да спазва критериите Europrivacy, зачитат същността на основните права и свободи на субектите на данни и не надхвърлят необходимото и пропорционалното в едно демократично общество за постигане на някоя от целите, изброени в член 23, параграф 1 от ОРЗД. Сертифицираният субект трябва да преразглежда оценката при всяка нормативна или организационна промяна, която би могла да възпрепятства спазването на критериите или да засегне обекта на оценката (ОНО) или правата на субектите на данни, като сертифициращият орган следва да бъде уведомяван за това (критерий Gl 1.1.1).

## **2.4 Общи задължения на администраторите и обработващите лични данни**

- 39 Критериите за сертифициране отразяват задълженията на администратора съгласно член 24 от ОРЗД (раздел Gl.4. от критериите) и съгласно тях се изисква договорните споразумения между обработващия личните данни и администратора да се оценяват в съответствие с член 28 от ОРЗД (раздел Gl.5 от критериите за сертифициране „Обработващи лични данни или подизпълнители, обработващи лични данни“) с цел да се гарантира, че обработващите лични данни, които участват в обработването на данни на ОНО, осигуряват същото ниво на защита на данните като нивото, което се изисква съгласно критериите Europrivacy. Във връзка с това ЕКЗД приветства различните критерии за сертифициране, свързани с ангажирането на подизпълнители, обработващи лични данни, като заявители, действащи в качеството на администратори или обработващи лични данни, тъй като това разграничение позволява по-добре да се отрази разпределението на ролите и отговорностите между участниците във веригата на обработване на данни (раздел Gl.5.1).
- 40 В критериите за сертифициране се изисква всички заявители да назначат длъжностно лице по защита на данните (ДЛЗД) дори в случаите, в които заявителят не е задължен да определи такова съгласно член 37 от ОРЗД. Съгласно критериите за сертифициране се проверява дали ДЛЗД отговаря на същите изисквания като тези, предвидени в членове 37—39 (раздел Gl.9 от критериите за сертифициране „Назначаване на длъжностно лице по защита на данните“), за да се гарантира, че ролята, функциите и квалификацията на длъжностното лице по защита на данните, което следи за съответствието на обработването на данни в ОНО, отговарят на „необходимите изисквания“. Във връзка с това Комитетът отбелязва, че назначаването на ДЛЗД не е задължително за администраторите и обработващите лични данни съгласно ОРЗД, освен ако са изпълнени условията, предвидени в член 37, параграф 1 от ОРЗД.
- 41 Съгласно критериите за сертифициране се изисква да се проверява съдържанието на регистрите на дейностите по обработване в съответствие с член 30 от ОРЗД (раздел G.5.3 от критериите „Регистри на дейностите по обработване“). Във връзка с това Комитетът приветства факта, че в критериите за сертифициране се поставя ясно изискване към заявителите да съдействат при отправени искания от страна на органите за защита на данните в ЕИП, които са компетентни по отношение на износителите, и да им предоставят при поискване регистъра на дейностите по обработване (критерий Gl.5.3.5).

## **2.5 Права на субектите на данни**

- 42 В критериите за сертифициране са разгледани правата на субектите на данни в съответствие с глава III от ОРЗД и е предвидено изискване за въвеждането на съответни мерки с цел да се гарантира, че при обработването в ОнО се зачитат правата на субектите на данни и се дава възможност за ефективното им упражняване. В раздел Gl.3 от критериите за сертифициране „Прозрачност на информацията, комуникация и начини за упражняване на правата на субекта на данни“ се предвижда, наред с другите гаранции, че субектите на данни имат право да бъдат информирани за обработването на данните и за начините, по които могат да упражняват правата си. ЕКЗД приветства по-специално факта, че в критериите за сертифициране се предвижда заявителят да разполага с процедури или механизъм за разглеждане на исканията на субектите на данни и, в случай че не се предприемат действия по искането на субектите на данни, да ги информира за причините за това, както и за правото им да подадат жалба пред орган за защита на данните в ЕИП и да потърсят средство за правна защита.

## **2.6 Технически и организационни мерки и оценка на рисковете за правата и свободите на субектите на данни**

- 43 Съгласно критериите за сертифициране се изисква прилагането на технически и организационни мерки, които да гарантират ниво на сигурност, съответстващо на риска, свързан с обработването, и които да осигуряват защита на данните на етапа на проектирането и по подразбиране в съответствие с членове 25 и 32 от ОРЗД (раздел Gl.6 от критериите за сертифициране „Защита на данните на етапа на проектирането и по подразбиране, както и сигурност на обработването“), с цел да се гарантира, че данните, обработвани в ОнО, са защитени по адекватен начин, както и че за тях се прилага защита на етапа на проектирането и по подразбиране. Освен това критериите за сертифициране включват раздел (а именно критерий Т относно технологичните и организационните мерки, проверките и контрола), в който подробно се разглеждат техническите и организационните мерки.
- 44 Съгласно критериите за сертифициране се изисква прилагането на мерки, които да гарантират, че задълженията за уведомяване при нарушение на сигурността на лични данни се изпълняват своевременно и с надлежащия обхват в съответствие с членове 33 и 34 от ОРЗД (раздел Gl.7 от критериите за сертифициране „Управление на нарушенията на сигурността на данните“).
- 45 Във връзка с това Комитетът отбелязва, че критериите за сертифициране включват подробен списък (критерий Gl.7.1.1. „Задължение за документиране на нарушенията на сигурността на данните“) относно информацията, която заявителят трябва да документира в случай на нарушение на сигурността на данните (например категориите лични данни, които са или биха могли да бъдат засегнати, приблизителния брой на засегнатите или потенциално засегнатите субекти на данни; категориите и приблизителното количество на записите на лични данни, които са засегнати или биха могли да бъдат засегнати, както и вероятните последици от нарушението на сигурността на личните данни). Освен това ЕКЗД приветства факта, че в критериите за сертифициране ясно се предвижда, че когато нарушението на сигурността на личните данни може да доведе до риск за правата и свободите на физическите лица, заявителят трябва да разполага с правила, процедура или механизъм за уведомяване на органа за защита на данните в ЕИП, който е компетентен по отношение на износителя(ите) и субектите на данни, в съответствие с изискванията на членове 33 и 34 от ОРЗД

(критерий Gl.7.1.2 „Задължение на администратора да уведомява и съобщава за нарушения на сигурността на данните“ и Gl 7.2 „Съобщение за нарушение на сигурността на личните данни на субекта на данните“).

- 46 ЕКЗД приветства също така факта, че съгласно критериите за сертифициране се изисква оценка на риска за правата и свободите на физическите лица, произтичащ от обработването на данни, обхванато от ОНО, като се предвижда участието на органа за защита на данните в ЕИП, който е компетентен по отношение на износителя(ите), в съответствие с член 35 от ОРЗД (раздел Gl.8. от критериите за сертифициране „Задължение да се прецени дали е необходима оценка на въздействието върху защитата на данните (DPIA)“).

## **2.7 Критерии за доказване на наличието на подходящи гаранции за предаването на лични данни**

- 47 Съгласно критериите за сертифициране се изисква да бъдат посочени всички предавания на лични данни към трети държави и към международни организации, участващи в ОНО, както и да се обоснове изборът на механизма за предаване на данни, който осигурява подходящи гаранции, съответстващи на предвидените в глава V от ОРЗД (раздел Gl.10 от критериите „Предаване на лични данни към трети държави или международни организации“). ЕКЗД потвърждава, че тези критерии ще се прилагат в случай на „по-нататъшно предаване“ на лични данни, включени в ОНО, към същата трета държава, в която се намира заявителят, или към друга трета държава. Комитетът приветства факта, че съгласно тези критерии на заявителя се поставя изрично изискване да разполага с ясно картографиране или регистър на всички потоци от лични данни в обхвата на ОНО, както и на установените предавания към трети държави и международни организации, и да приеме подходящото правно основание за предаване на личните данни в съответствие с предвиденото в глава V от ОРЗД, като се съобрази със задължението да не подкопава нивото на защита на личните данни, предвидено в рамките на ЕИП.
- 48 ЕКЗД отбелязва също, че съгласно критериите за сертифициране от заявителя се изисква да е извършил оценка на въздействието на предаването и, при необходимост, да е приел допълнителни мерки, за да гарантира, че нивото на защита на прехвърлените данни не се нарушава (критерий Gl.10.1.5).

## **3 Допълнителни критерии за Европейския печат за защита на данните, който да се използва като инструмент за предаване на данни**

- 49 Съгласно Насоките относно сертифицирането като инструмент за предаване на данни схемата за сертифициране следва да гарантира, че вносителят на данни „е оценил правилата и практиките на третата държава, в която осъществява дейност, или това дали те не го възпрепятстват да спазва поетите по силата на сертифицирането ангажименти“. Във връзка с това Комитетът отбелязва, че в критерий ADI.2.1.5 се определят условията, които заявителите трябва да изпълнят при определянето на ОНО по време на разглеждането на заявлението им за сертифициране. По-конкретно, преди да разгледа възможността за провеждане на сертифициращ одит, сертифициращият орган трябва да провери дали заявителят е в състояние да докаже, че „законодателството и практиката на третата държава не възпрепятстват спазването на

изискванията за сертифициране“. Ако това не е така, процесът на сертифициране ще бъде преустановен още на етапа на подаване на заявлението.

- 50 Комитетът отбелязва също така, че съгласно критерий Gl.11.1.3 заявителят следва да анализира законодателството и практиките в третата държава и да определи потенциалното въздействие върху правата и свободите на субекта на данни, чиито данни може да са обект на внасяне, както и да разполага с „правила, процедури или политики за предоставяне на неговия писмен анализ на местното законодателство и практики на разположение на сертифициращия орган и на компетентните органи за защита на данните при поискване“.
- 51 Освен това, съгласно Насоките за сертифицирането като инструмент за предаване на данни, в критериите за сертифициране се предвижда, че при необходимост заявителят трябва да е приел допълнителни мерки, за да гарантира, че нивото на защита на предаваните лични данни не се нарушава, а когато това не е възможно, вносителят на данните трябва да уведоми износителя на данните и предаването на лични данни следва да бъде временно преустановено или прекратено (критерий Gl 11.1.3).
- 52 Освен това Комитетът отбелязва, че в съответствие с член 42, параграф 2 от ОРЗД в схемата Europrivacy се предвижда, че преди извършването на каквото и да е предаване на данни между вносителя и износителя на данни следва да бъде сключен договор, който да съдържа съответните обвързващи и подлежащи на изпълнение ангажименти, и е представен образец на такъв договор. Във връзка с това ЕКЗД отбелязва, че в съответствие с Насоките за сертифицирането като инструмент за предаване на данни критериите за сертифициране включват подробен списък на съдържанието на обвързващите и подлежащи на изпълнение ангажименти, които следва да бъдат поети от заявителя по отношение на всеки износител в ЕИП, сред които задължението да признае правото на субектите на данни, като трети страни бенефициери, да налагат спазването на правилата по сертифицирането спрямо вносителя на данни, притежаващ сертификат, да сътрудничи на органите за защита на данните в ЕИП, които са компетентни по отношение на износителите на данни (включително като приема техните одити и инспекции, съобразява се с техните съвети и спазва техните решения), да спазва всяко задължително решение, постановено в юрисдикцията и съдилищата на държавите — членки на ЕИП, във връзка със сертифицирането, да обработва получените данни само докато сертификатът е валиден, да върне и/или да заличи получените данни, ако сертификатът бъде отнет. В критериите за сертифициране се предвижда също, че заявителят следва да гарантира, че няма основания да счита, че законодателството и практиките в третата държава, приложими към обработването в Оно, включително евентуални изисквания за разкриване на лични данни или мерки, разрешаващи достъп на публични органи, го възпрепятстват да изпълнява ангажиментите си по сертифицирането, както и да информира износителя на данни за всички относими промени в законодателството или практиката в това отношение (критерий Gl.11.1.1 „Обвързващи и подлежащи на изпълнение ангажименти за вносителите на данни“).

## 4 Заключение/препоръки

- 53 В заключение ЕКЗД счита, че критериите за сертифициране Europrivacy, предназначени да се използват като инструмент за предаване на данни, са в съответствие с ОРЗД и ги одобрява в изпълнение на задачата на Комитета, определена в член 70, параграф 1, буква о) от ОРЗД, което води до общо сертифициране (Европейски печат за защита на данните), което да се използва като инструмент за предаване на данни.

- 54 ЕКЗД счита, че критериите за сертифициране представляват неразделна част от схемата за сертифициране, и ще впише схемата за сертифициране Europrivacy в публичния регистър на механизмите за сертифициране и печатите и маркировките за защита на данните, като ще направи критериите обществено достъпни в съответствие с член 42, параграф 8 от ОРЗД.

## **5 Заключение и бележки**

- 55 Настоящото становище е предназначено за НО — Люксембург, и ще бъде публикувано съгласно член 64, параграф 5, буква б) от ОРЗД.

За Европейския комитет по защита на данните

Председател

Anu Talus